REMARKS/ARGUMENTS

Claims 1-12 and 14-20 are currently amended as shown above. Claims 1-20 are currently pending in the application.

Provisional obviousness-type double patenting rejection:

A terminal disclaimer in compliance with 37 C.F.R. 1.321(c) or 1.321(d) is being filed herewith by the registered attorney of record in accordance with 37 C.F.R. 3.73(b).

Rejections under 35 U.S.C. §102(b):

The Examiner has rejected claims 1-20 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,292,896 to Guski et al ("Guski"). Amended claim 1 recites in part:

> "[...]providing a previous encryption key;
> selecting an old data record from the plurality of data records; and
> regenerating a new encryption key at a user node as a function of the previous encryption key and the old data record."

With respect to claim 1, the Examiner has referred to Guski at col. 9, lines 11-34, 44-54, for the proposition that it teaches or discloses "selecting encrypted data; and regenerating a new encryption key at a node with an encryption key and selected encrypted data." As shown above, claim 1 has been amended to clarify that the new encryption key is regenerated at the user node as a function of the previous encryption key and the old data record.

For its part, the cited passages of Guski teach a key weakening function, which is a method for deriving a weakened session key (KS) from a strong key (K'). As noted by Guski, this method involves passing the original value K' through a plurality of functions, including a non-key-bit set function, a one-way function, a key-bit-select function and a randomized key-

select function. The first three functions create intermediate keys from the original value K', and the fourth function, operating on the third intermediate value, creates the weakened session key KS.

However, Guski does not teach or disclose regenerating a new encryption key as a function of a previous encryption key and an old data record, as recited in amended claim 1. On the contrary, Guski specifically teaches the use of a multitude of functions operating in a linear fashion on a single input value, i.e. the original value K', the first intermediate key, the second intermediate key, and the third intermediate key. As Guski does not teach or disclose each and every limitation of amended claim 1, the applicant respectfully submits that claim 1, and its dependents 2-18, are in condition for allowance.

With respect to amended claim 19, the Examiner has provided the same passages from Guski as teaching "means for regenerating a new encryption key as a function of the previous encryption key and an old data record." To the extent that this recitation from amended claim 19 is similar to amended claim 1, the Applicant respectfully submits that the arguments provided above are equally applicable herein. In particular, as noted above, Guski teaches a single input value K' for producing the weakened session key KS. In contrast, amended claim 19 recites regenerating a new encryption key as a function of the previous encryption key and an old data record." As Guski does not teach or disclose using an old data record as an input into the key-weakening steps recited therein, the Applicant respectfully submits that claim 19 and its dependent claim 20 are also in condition for allowance.

Conclusion:

Claims 1-12 and 14-20 have been amended as shown above, and claims 1-20 are currently pending. In view of the current amendments and arguments presented above, the Applicant hereby requests the allowance of claims 1-20. However, should the Examiner have any comments, the undersigned would welcome a telephone call in order to expedite placement of the application into condition for allowance.

Respectfully submitted,

Robert W. Becker, Reg. 26,255
Attorney for Applicant(s)

ROBERT W. BECKER & ASSOCIATES
707 State Hwy 333, Ste. B   Telephone: 505 286 3511
Tijeras, New Mexico 87059-7507   Telefax: 505 286 3524